Konfigurieren von RADIUS KeyWrap in ISE

Inhalt

Einleitung

Voraussetzungen

Verwendete Komponenten

Hintergrundinformationen

Konfigurieren

- ISE
- Switch
- PC

Überprüfung

Häufig gestellte Fragen

Referenz

Einleitung

In diesem Dokument wird das Verfahren zum Konfigurieren von RADIUS KeyWrap in der Cisco ISE und dem Cisco Switch beschrieben.

Voraussetzungen

- Kenntnisse von dot1x
- Kenntnisse des RADIUS-Protokolls
- Kenntnisse des EAP

Verwendete Komponenten

- ISE 3.2
- Cisco C9300-24U mit Softwareversion 17.09.04a
- Windows 10-PC

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Schlüsselumbruch ist eine Technik, bei der ein Schlüsselwert mit einem anderen Schlüssel verschlüsselt wird. Der gleiche Mechanismus wird in RADIUS zur Verschlüsselung des

Schlüsselmaterials verwendet. Dieses Material wird in der Regel als Nebenprodukt einer EAP-Authentifizierung (Extensible Authentication Protocol) erstellt und nach einer erfolgreichen Authentifizierung in der Access-Accept-Nachricht zurückgegeben. Diese Funktion ist erforderlich, wenn ISE im FIPS-Modus ausgeführt wird.

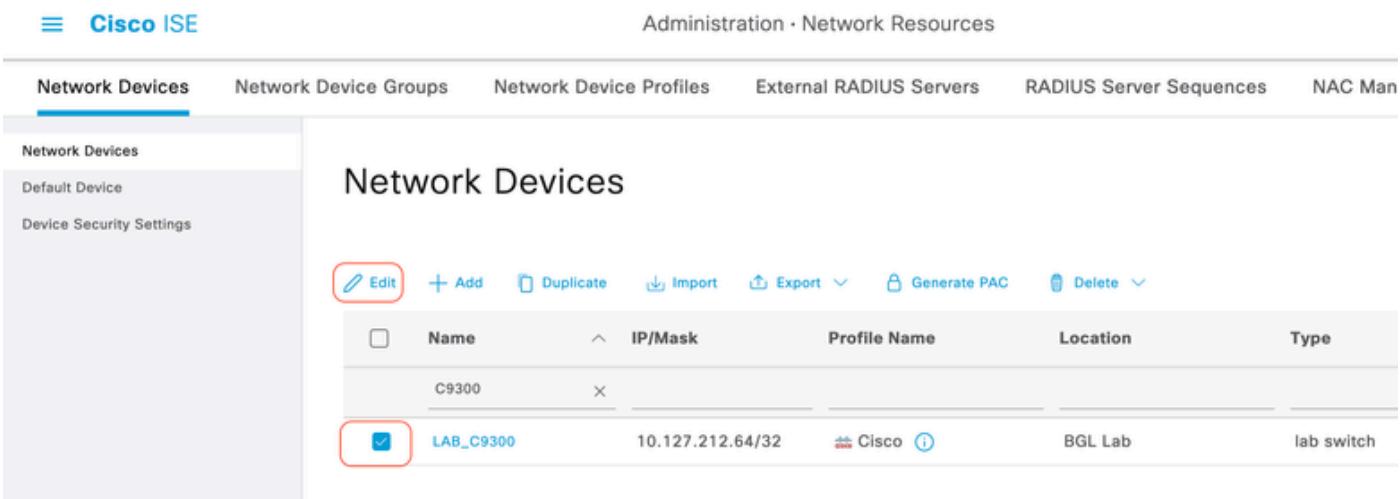
Dadurch wird eine Schutzschicht geschaffen, die das eigentliche Schlüsselmaterial zur Absicherung gegen potenzielle Angriffe isoliert. Das zugrunde liegende Kernmaterial ist für die Angreifer praktisch unzugänglich, selbst wenn die Daten abgefangen werden. RADIUS-Schlüsselverpackungen sollen in erster Linie verhindern, dass wichtige Materialien, die digitale Inhalte sichern, insbesondere in einem großen Netzwerk auf Unternehmensebene veröffentlicht werden.

In der ISE wird der Schlüsselverschlüsselungsschlüssel verwendet, um die Schlüsselmaterialien mit der AES-Verschlüsselung und dem Nachrichtenauthentifizierer-Schlüsselschlüssel getrennt vom gemeinsamen geheimen RADIUS-Schlüssel zu verschlüsseln, um Nachrichtenauthentifizierer-Code zu generieren.

Konfigurieren

ISE

Schritt 1: Navigieren Sie zu Administration > Network Resources > Network Devices. Klicken Sie auf das Kontrollkästchen für das Netzwerkgerät, für das Sie RADIUS KeyWrap konfigurieren möchten. Klicken Sie auf Bearbeiten (wenn das Netzwerkgerät bereits hinzugefügt wurde).



Phase 2: Erweitern Sie die RADIUS-Authentifizierungseinstellungen. Klicken Sie auf das Kontrollkästchen KeyWrap aktivieren. Geben Sie den Schlüssel für die Verschlüsselung und den Schlüssel für den Nachrichtenauthentifizierer ein. Klicken Sie auf Speichern.

General Settings

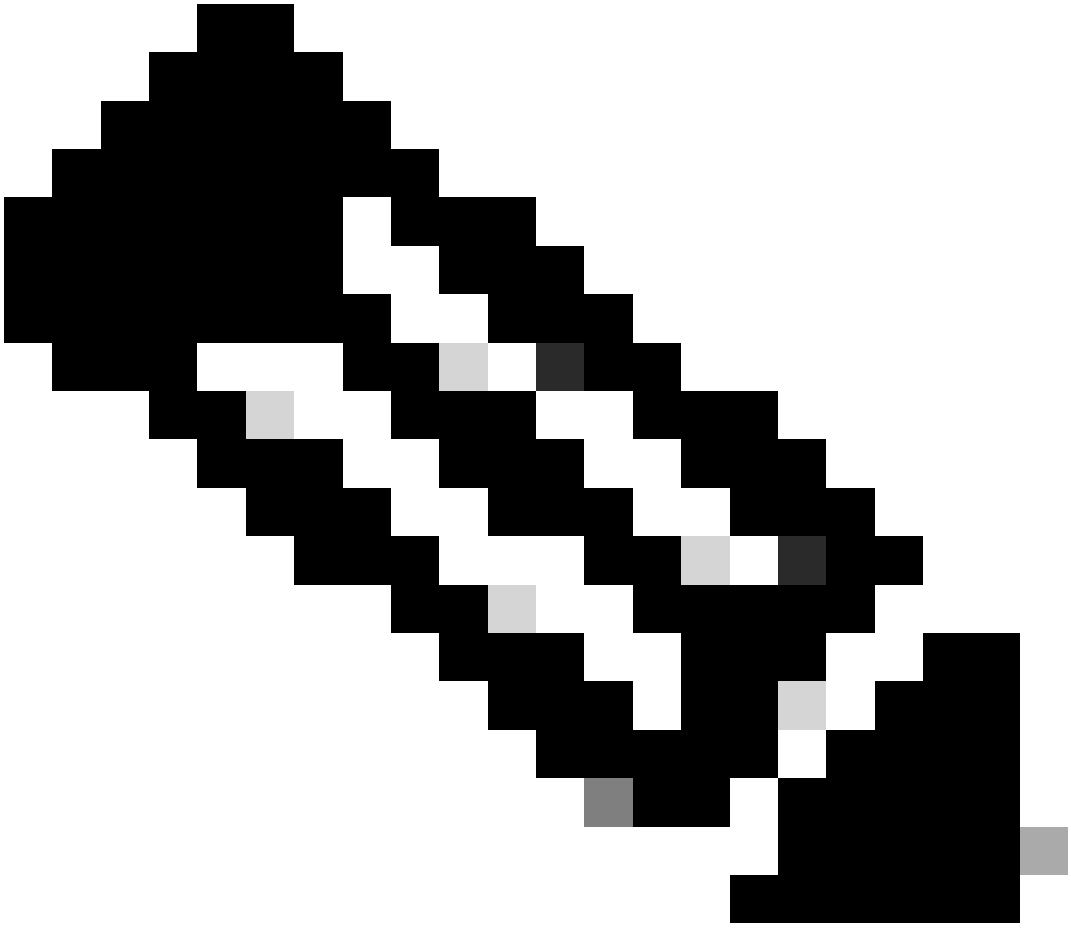
Enable KeyWrap

Key Encryption Key 22AB0###CA#1b2b1 Hide

Message Authenticator Code Key 12b1CcB202#2Cb1#bCa# Hide

Key Input Format

ASCII HEXADECIMAL



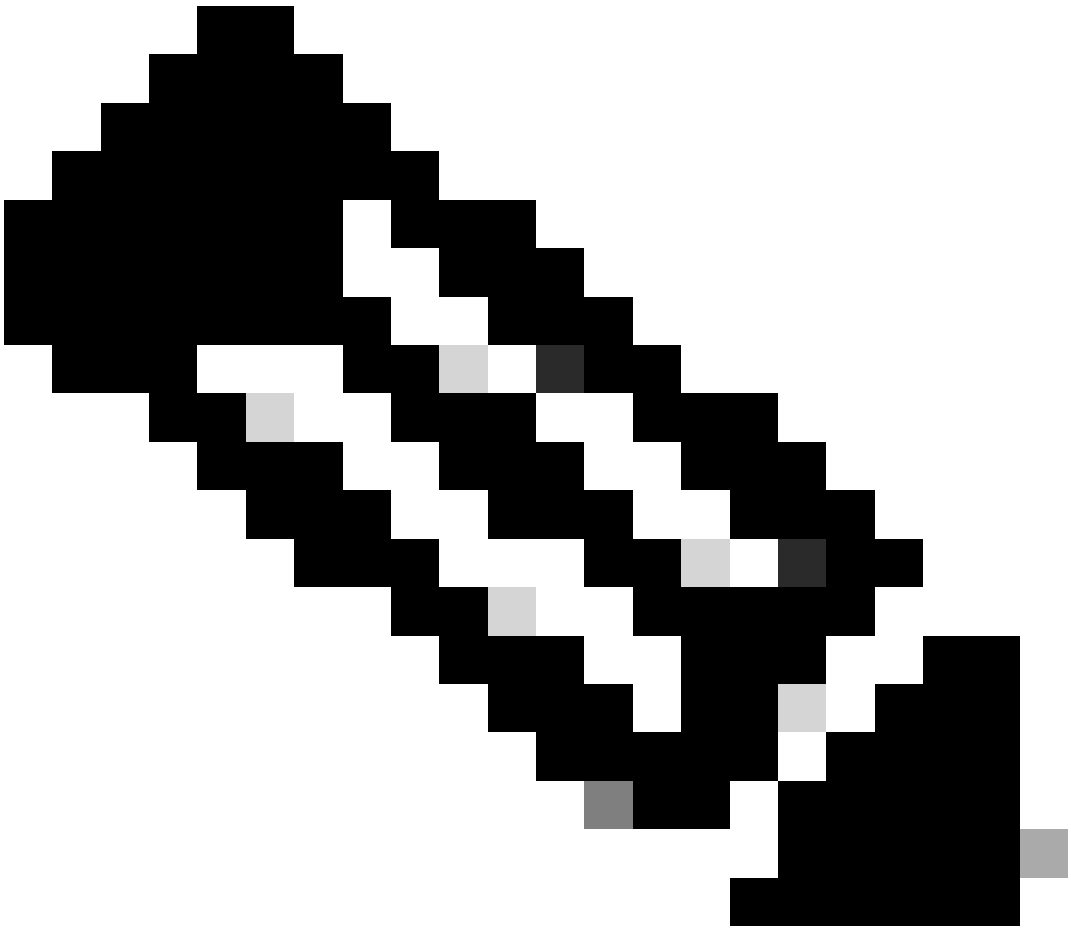
Hinweis: Der Schlüssel für den Verschlüsselungsschlüssel und der Schlüssel für den Nachrichtenauthentifizierer müssen unterschiedlich sein.

Switch

AAA-Konfiguration im Switch zur Aktivierung der RADIUS KeyWrap-Funktion.

```
aaa authentication dot1x default group RADGRP
aaa authorization network default group RADGRP
aaa accounting dot1x default start-stop group RADGRP

radius server ISERAD
 address ipv4 10.127.197.165 auth-port 1812 acct-port 1813
 key-wrap encryption-key 0 22AB0###CA#1b2b1 message-auth-code-key 0 12b1CcB202#2Cb1#bCa# format ascii
 key Iselab@123

aaa group server radius RADGRP
 server name ISERAD
 key-wrap enable
```

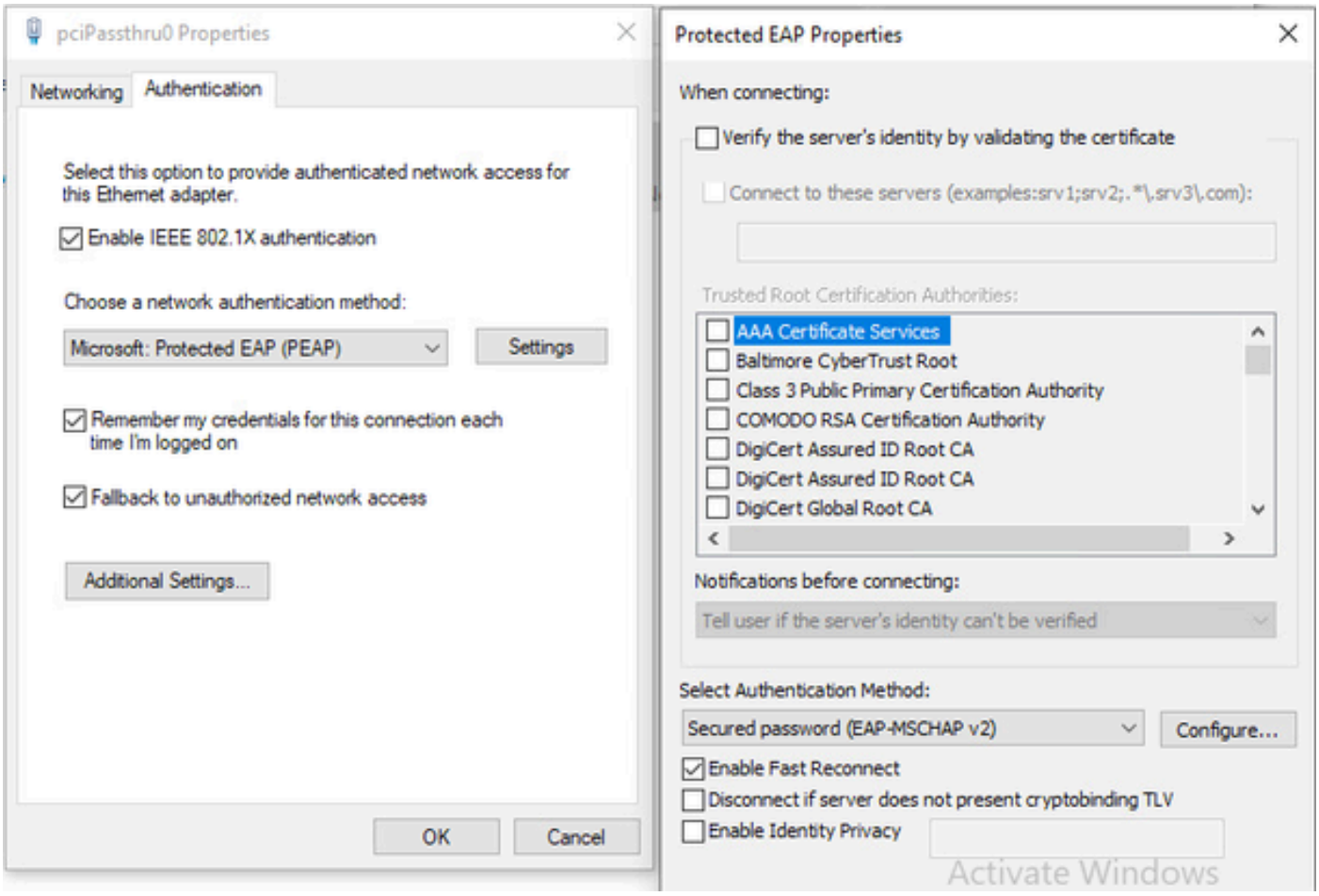
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



Anmerkung: Der Verschlüsselungsschlüssel muss 16 Zeichen lang und der Nachrichtenauthentifizierungscode 20 Zeichen lang sein.

PC

Für PEAP-MSCHAPv2 konfigurierte Windows 10-Komponente.



Überprüfung

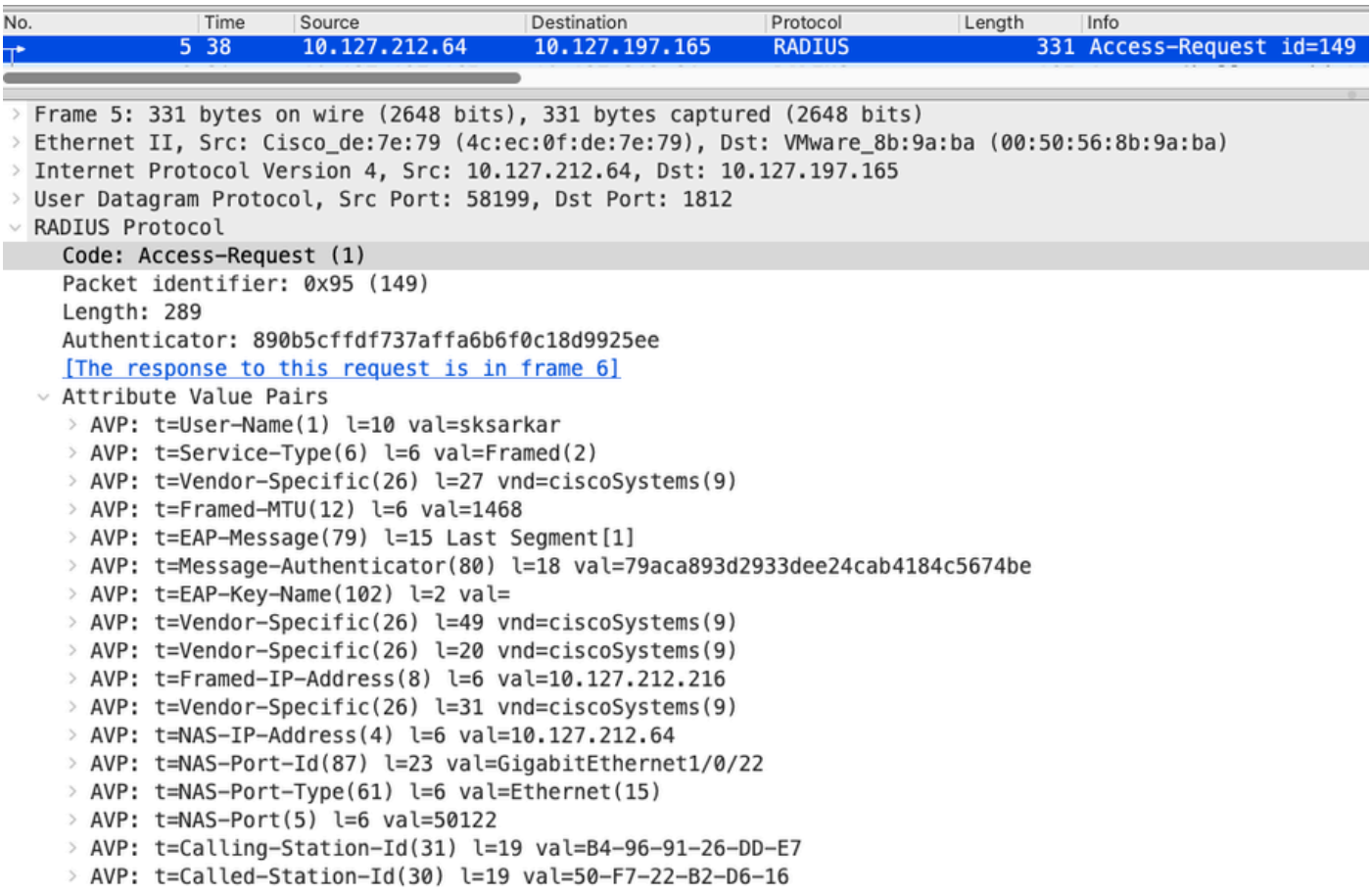
Wenn die RADIUS KeyWrap-Funktion auf dem Switch nicht aktiviert ist:

show radius server-group <NAME DER SERVERGRUPPE>

In der Befehlsausgabe muss Keywrap aktiviert sein: FALSCH.

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: FALSE
```

In der Paketerfassung können Sie sehen, dass es kein Cisco-AV-Pair-Attribut für App-Key, Random-Nonce und separaten Nachrichten-Authentifikator-Code gibt. Dies zeigt an, dass RADIUS KeyWrap auf dem Switch deaktiviert ist.

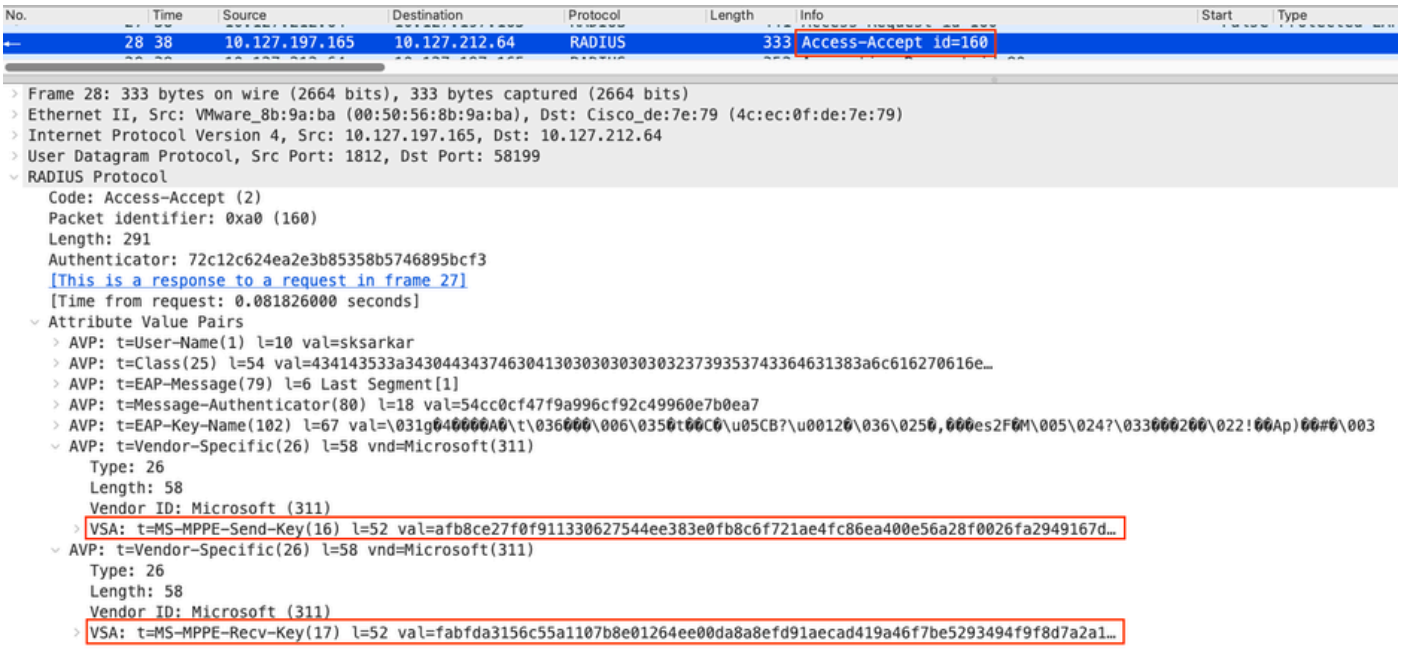


In der Datei ISE port-server.log können Sie sehen, dass ISE nur das Integritätsattribut überprüft, das Message-Authenticator ist.

```
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
[8] Framed-IP-Address - value: [10.127.212.216]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[80] Message-Authenticator - value: [<88>/`f

       |

        >

         <18><06>(
```

```
          ?


            ]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A0000002B9E06997E]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=292332370] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
```

Im Access-Accept-Paket können Sie sehen, dass der MS-MPPE-Send-Key und der MS-MPPE-Recv-Key vom RADIUS-Server an den Authenticator gesendet werden. MS-MPPE gibt das Schlüsselmaterial an, das von den EAP-Methoden generiert wird und zur Datenverschlüsselung zwischen Peer und Authenticator verwendet werden kann. Diese 32-Byte-Schlüssel werden aus dem gemeinsamen RADIUS-Schlüssel, dem Request-Authentifizierer und einem zufälligen Salz abgeleitet.



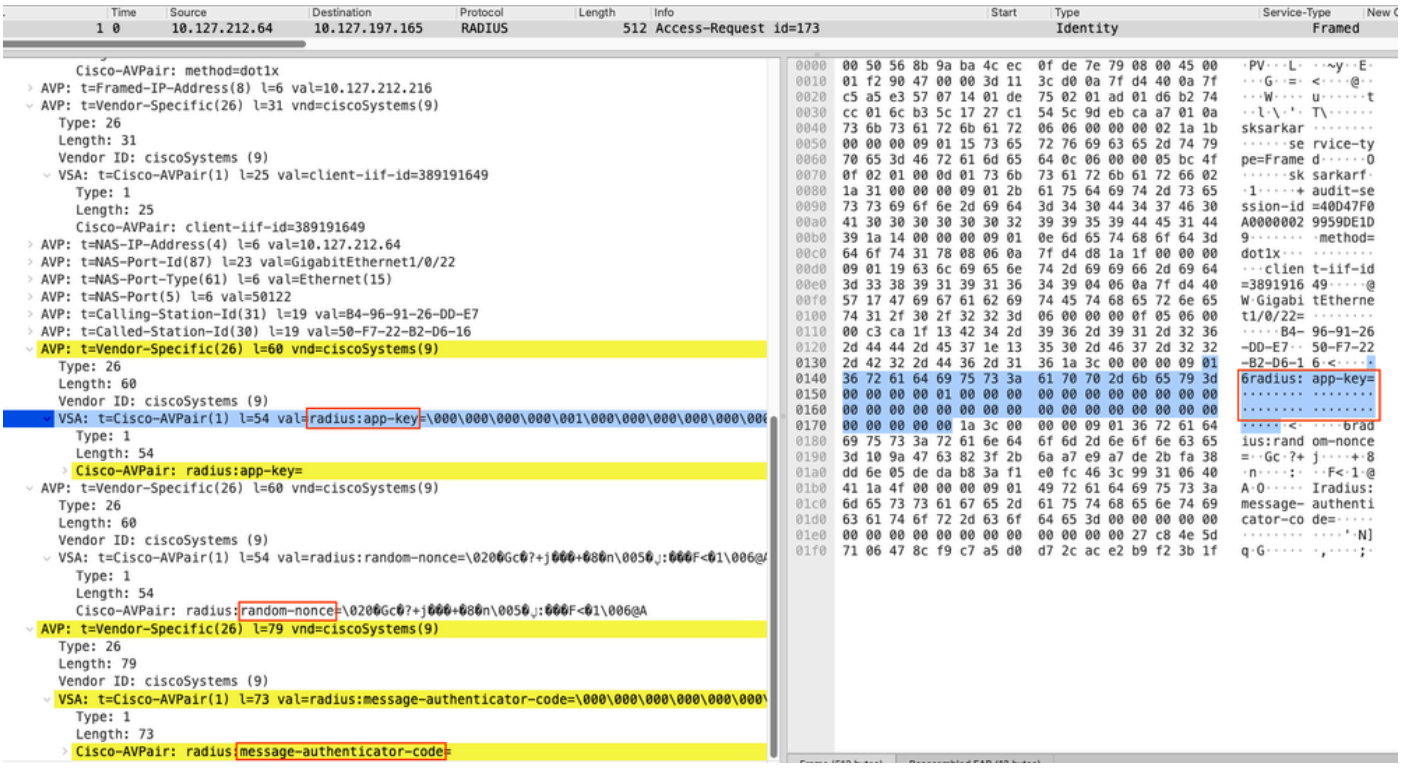
Wenn die RADIUS KeyWrap-Funktion auf dem Switch und der ISE aktiviert ist:

show radius server-group <NAME DER SERVERGRUPPE>

In der Befehlsausgabe muss Keywrap aktiviert sein: WAHR.

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: TRUE
```

Bei der Paketerfassung sehen Sie, dass ein Cisco-AV-Pair-Attribut für den App-Schlüssel (ohne Daten) vorhanden ist, Random-Nonce und ein separater Message-Authentifikator-Code vorhanden sind. Dies weist den RADIUS-Server darauf hin, dass der Authenticator (Switch) den RADIUS KeyWrap unterstützt und der Server diesen verwenden muss.

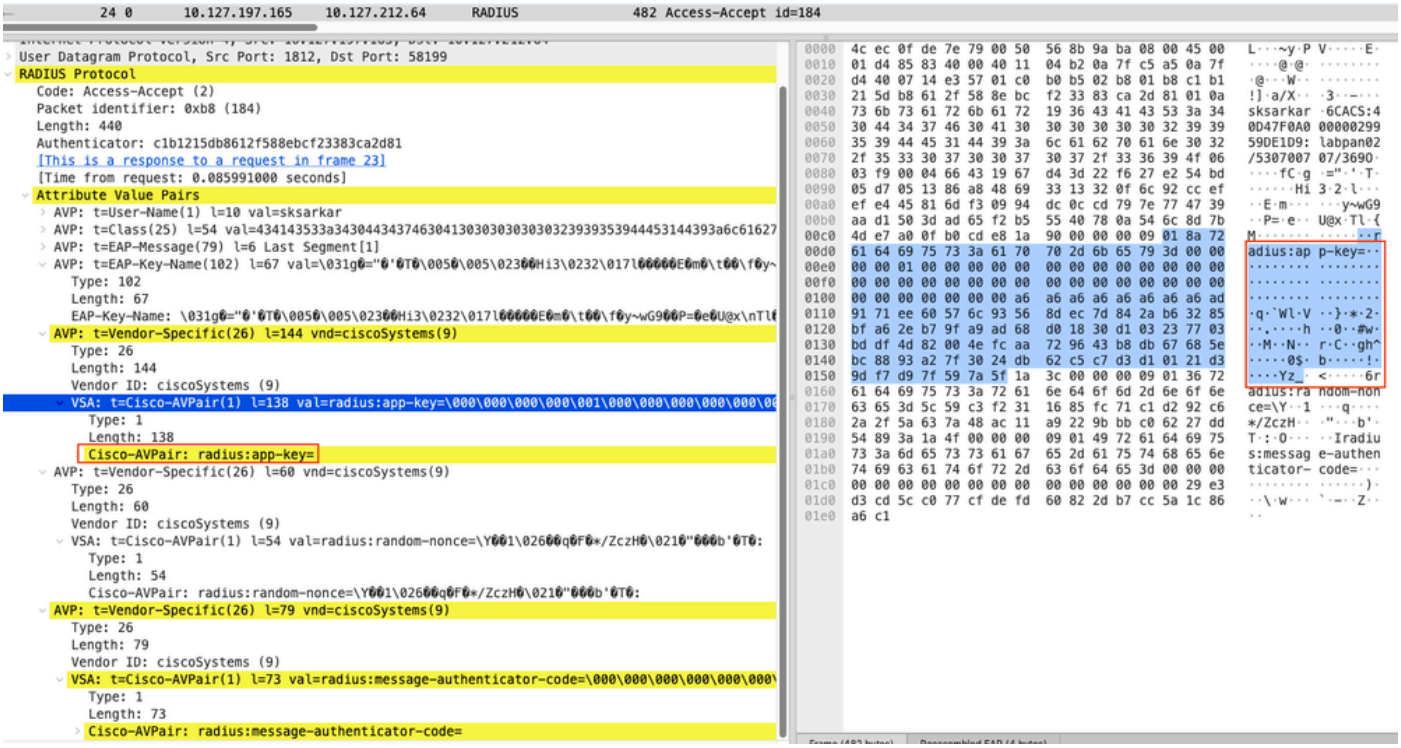


In der Datei ISE prt-server.log können Sie sehen, dass die ISE den Attribute-App-Key validiert und dass random-nonce und Message-Authenticator-Code im ACCESS-REQUEST-Paket enthalten waren.

```
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
```

```
[6] Service-Type - value: [Framed]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A000000319E1CAEFD]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=293712201]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
```

Im Access-Accept-Paket können Sie sehen, dass die verschlüsselten Schlüsselmaterialien im app-key-Attribut zusammen mit einem random-nonce- und einem Message-Authenticator-Code enthalten sind. Diese Attribute sind sicherer und flexibler als die aktuell definierten anbieterspezifischen MS-MPPE-Send-Key- und MS-MPPE-Recv-Key-Attribute.



Häufig gestellte Fragen

1) Muss RADIUS KeyWarp sowohl auf dem Netzwerkgerät als auch auf der ISE aktiviert werden, damit es funktioniert?

Ja, RADIUS KeyWrap muss sowohl auf dem Netzwerkgerät als auch auf der ISE aktiviert sein, damit es funktioniert. Wenn Sie KeyWrap zwar nur auf der ISE, aber nicht auf dem Netzwerkgerät aktivieren, funktioniert die Authentifizierung dennoch. Wenn Sie die Funktion jedoch auf einem Netzwerkgerät, aber nicht in der ISE aktiviert haben, schlägt die Authentifizierung fehl.

2) Erhöht die Aktivierung von KeyWrap die Ressourcenauslastung auf der ISE und dem Netzwerkgerät?

Nein, die Ressourcenauslastung auf der ISE und dem Netzwerkgerät nimmt nach der Aktivierung von KeyWrap nicht wesentlich zu.

3) Wie viel zusätzliche Sicherheit bietet RADIUS KeyWrap?

Da der RADIUS selbst keine Verschlüsselung für seine Nutzlast bereitstellt, bietet KeyWrap zusätzliche Sicherheit durch Verschlüsselung der Schlüsselmaterialien. Das Sicherheitsniveau hängt davon ab, welcher Verschlüsselungsalgorithmus zur Verschlüsselung des Schlüsselmaterials verwendet wird. In der ISE wird AES verwendet, um das Schlüsselmaterial zu verschlüsseln.

Referenz

- Anbieterspezifische RADIUS-Attribute von Cisco für die Bereitstellung von Schlüsselmaterial

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.